REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims 1-5, 7-8 and 10-34 are pending in the application, with claims 1, 11, and 23 being independent. Claims 6 and 9 were previously canceled without prejudice to or disclaimer of the subject matter recited therein. Claims 1-5, 7-8 and 10-34 are amended herein. Support for the claim amendments and additions can be found in the original disclosure. No new matter has been added.

35 U.S.C. §103 Rejections

Claims 1-5, 7-8 and 10-22 stand rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 5781773 to Vanderpool, et. al. ("Vanderpool") in view of U.S. Patent No. 6684326 to Cromer, et al. ("Cromer"). (See Office Action p. 3)

Claims 23-25, 27-30 and 32-34 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6615329 to Scott, et. al. ("Scott") in view of U.S. Patent No. 7237126 to Neufeld, et al. ("Neufeld"). (See Office Action p. 11)

Claims 26 and 31 stand rejected under 35 U.S.C. § 103(a) as being obvious over Scott in view of Neufeld and in further view of Cromer. (See Office Action p. 15)

Applicant respectfully traverses these rejections. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance

of the application, claims 1-5, 7-8 and 10-34 has been amended and are believed to be patentable over the cited references.

Amended Independent claim 1, as presently presented, is directed to a method of file system protection for a resource-sparing operating system image, and recites, among other things, "loading in a client device a first image of the resource-sparing operating system (OS) that includes processor instructions into random access memory (RAM), the first image including an embedded second image of a catalog file comprising client device attributes," "extracting a second hash from the second image of the catalog file;" and "validating the use of the first image to boot the computing device if the first hash and the second hash match."

Independent claim 11, as presently presented, is directed to a method of file system protection for a resource-sparing operating system image, and recites, among other things, "comparing information extracted from the embedded catalog file image with information obtained from the resource-sparing OS image to determine if the resource-sparing OS image is a properly released resource-sparing OS image."

Vanderpool is directed to a method for storing data for search and display and discloses storing compressed images and text supplements in a subdirectory location, where the location name is in part based on a hash algorithm. The hash algorithm is any algorithm used to generate a random number that can be used to provide random placement of the compressed images and text supplements in the subdirectory. (Office Action pages 3-4)

However, Vanderpool fails to disclose or suggest "loading in a client computing device a first image of the resource-sparing OS image that includes processor instructions", "a first image including an embedded second image of a catalog file comprising client device attributes" and "extracting a second hash from the second image" as recited in claim 1. Further Vanderpool fails to disclose or suggest "comparing information extracted from the embedded catalog file with information obtained from the resource sparing OS," as presently recited in independent claim 11.

Cromer was cited for its alleged teaching of a "system for performing an authenticated boot of a computer system," and "comparing a decrypted received hash to a list of authorized operating system boot hashes so that the system boots or halts appropriately." (Office Action, page 4).

However, Cromer fails to remedy the deficiencies in Vanderpool noted above with respect to claim 1 and 11. For example, Cromer fails to disclose or suggest "loading in a client computing device a resource-sparing OS image that includes processor instructions", "a first image including an embedded second image of a catalog file comprising client device attributes", "extracting with the client computing device a second hash from the second image" and "extract a second hash from the second image of the catalog file," (emphasis added) as presently recited in amended claim 1.

Further, Cromer fails to remedy the deficiencies in Vanderpool noted above with respect to claim 11. For example, Cromer fails to disclose or suggest

"comparing information extracted from the embedded catalog file with information obtained from the resource sparing OS," or "blocking use of the resource-sparing OS image to boot the computing device..." as presently recited in amended claim 11.

Vanderpool is directed to a method for storing data in a standalone client computer subdirectory. Cromer is directed to a method of authenticating boot operations on a server of a networked computer. Each reference is directed to a different type of computer system (networked server vs. standalone). Applicant submits that there is no suggestion, teaching, or reason given by any one of the cited references that would give one of ordinary skill in the art reason to combine Cromer with the teachings of Vanderpool to obtain the applicants claimed invention. Further, Vanderpool and Cromer, whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 1 or 11. Accordingly, amended independent claims 1 and 11 are allowable.

Dependent claims 2-5, 7-8, 10 and dependent claims 12 - 22 depend from independent claims 1 and 11, respectively, and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Independent claim 23, as presently presented, is directed to a portable computing device, and recites, among other things:

"the cryptographic module of the bootloader is operative to examine an update image to the OS image to determine if the update image should be programmed into the unprotected area of flash memory to boot the computing device, wherein a signed catalog image is an image of a signed catalog file and is embedded in the update image, wherein the signed catalog file is derived by signing a catalog file and wherein the cryptographic module is operative to program the update image into the unprotected area of flash memory boot the computing device based on a determined relationship between information extracted from the embedded signed catalog file and one of information about the components of the computing device and information determined from the update image."

Scott is directed to a method for controlling access to a protected area of memory. Scott includes instructions that set a write authorization flag as part of a boot loader. The memory in Scott may have a protected area (that may be part of a processor) and an unprotected area. Access to the protected area is typically controlled by a voltage level of a memory input pin. Scott discloses checking the state of the authorization flag to determine whether write to the protected area is authorized.

However, Scott fails to disclose or suggest a "cryptographic module" as recited in claim 23. Scott also fails to disclose or suggest determining if an updated image should be stored in an unprotected area of flash memory based on a determined relationship between the information extracted from the embedded signed catalog file and stored in the update image as recited in amended claim 23..

Neufeld was cited for its alleged teaching of protection of reprogrammable start up memory ... from unauthorized reprogramming or alteration. (Office Action, page 12) Neufeld checks an authenticity and operability of firmware using a digital

signature. Operability means that "the firmware was indeed signed by some trusted entity and the firmware is intact." (Emphasis added) (Neufeld, 4:40-48)

However, Neufeld fails to remedy the deficiencies in Scott noted above with respect to claim 23. For example, Neufeld fails to disclose or suggest a cryptographic module that is "operative to program the update image into the unprotected area of flash memory boot the computing device based on a determined relationship between information extracted from the embedded signed catalog file and one of information about the components of the computing device and information determined from the update image" (emphasis added) as presently recited in amended claim 23.

Applicant submits that there is no suggestion, teaching, or reason given by any one of the cited references that would give one of ordinary skill in the art reason to combine Neufeld with the teachings of Scott. Further, Neufeld and Scott, whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 23. Accordingly, as discussed during the interview, amended independent claim 23 is allowable.

Dependent claims 24-34 depend from independent claim 23, respectively, and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

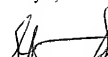
CONCLUSION

For at least the foregoing reasons, it is respectfully submitted that claims 1-5, 7-8 and 10-34 are in condition for allowance. Applicant respectfully requests reconsideration and withdrawal of the rejections and an early notice of allowance.

If any issue remains unresolved that would prevent allowance of this case, **Applicant requests that the Examiner contact the undersigned attorney to resolve the issue**.

Respectfully Submitted,

Lee & Hayes, PLLC

Dated: 7/29/08 By: 

Steven C. Stewart
Reg. No. 33555
206-315-7909